UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/775,537	02/09/2004	Brian Hernacki	68865.001203	6706

69417 7590 03/22/2010

HUNTON & WILLIAMS LLP / SYMANTEC CORPORATION
INTELLECTUAL PROPERTY DEPT.
1900 K STREET, NW
SUITE 1200
WASHINGTON, DC 20006-1109

EXAMINER	
TRAN, TUNG Q	

ART UNIT	PAPER NUMBER
2473	

MAIL DATE	DELIVERY MODE
03/22/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/775,537	HERNACKI, BRIAN	
	Examiner	Art Unit	
	Tung Q. Tran	2473	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12/11/2010*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3-5,7,8,10-16 and 18-24* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3-5,7,8,10-16 and 18-24* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 101

1. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

2. Claim 21 is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claim 21 recites "A computer readable storage medium..." but the specification discloses that "medium such as a computer readable storage medium or a computer network wherein program instructions are sent over optical or electronic communication links" in page 5, lines 3-5. That means "medium" of claim 21 can be transitory propagating signals *per se*, therefore, claim 21 is rejected under 35 US.C. § 101 as covering non-statutory subject matter. *See In re Nuijten*, 500 F.3d 1346, 1356-57 (Fed. Cir. 2007) (transitory embodiments are not directed to statutory subject matter) and *Interim Examination Instructions for Evaluating Subject Matter Eligibility Under* 35 *Us.* C. § *101*, Aug. 24, 2009; p. 2. Current USPTO practice suggests that a claim drawn to such a computer readable medium that covers both transitory and non-transitory embodiments may be amended to narrow the claim to cover only statutory embodiments to avoid a rejection under 35 U.S.C. § 101 by adding the limitation "non-transitory" to the claim. Such an amendment would typically not raise the issue of new matter, even when the specification is silent because the broadest reasonable interpretation relies on the ordinary and customary meaning that includes signals *per*

se. The limited situations in which such an amendment could raise issues of new matter occur, for example, when the specification does not support a non-transitory embodiment because a signal *per se* is the only viable embodiment such that the amended claim is impermissibly broadened beyond the supporting disclosure. *See, e.g., Gentry Gallery, Inc.* v. *Berkline Corp.*, 134F.3d 1473 (Fed. Cir. 1998).

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1, 3-5, 8, 16, 18-21, 23 are rejected under 35 U.S.C. 102(e) as being anticipated by Pochon et al. (US 2003/0048793).

Pochon discloses method and apparatus for data normalization comprising the following features.

Regarding claims 1, 20, and 21, a method/system/computer readable storage medium comprising computer instructions for assembling fragmented network traffic (see method, apparatus, and computer readable medium for assembling fragmented network traffic recited in the abstract; Fig. 1-7, 10-11), comprising: detecting, by a monitoring node, an anomaly in the fragmented network traffic whereby two or more

fragments within the fragmented network traffic have overlapping offsets (see [0019-0026]; [0089]-[0093], [0093], where an NIDS checks to determine whether there is a conflict between received fragments whereby two or more fragments have overlapping offset; also see Fig. 3-4); performing a query to determine configuration information associated with how a destination node to which the two or more fragments are addressed is configured to reassemble overlapping fragments (see querying normalization table to determine information that is associated with how a end-system/host to which the two or more fragments are addressed is configured to reassembly overlapping fragments recited in [0051-0055]; [0089-0093]; Fig. 1-7, 10-11; [0019-0026]); and reassembling the two or more fragments according to the configuration information associated with the destination node (see assembling fragments recited in the abstract; [0050]; claims 1 and 14; [0019-0026]; Fig. 1-7, 10-11).

Regarding claim 3, wherein determining that said two or more fragments overlap comprises reading a header value associated with one of the fragments (see [0051-0055]; [0089-0093]; Fig. 1-7, 10-11; [0019-0026]).

Regarding claim 4, wherein the header value comprises an offset value (see [0091]-[0092]).

Regarding claims 5 and 19, wherein detecting an anomaly comprises determining that said two or more fragments overlap and that at least two of said fragments comprise different data for an overlapping portion of said fragments ([0051-0055]; [0089-0093]; Fig. 1-7, 10-11; [0019-0026]).

Regarding claims 8 and 23, querying a information base (see querying normalization table to determine information that is associated with how a end-system/host to which the two or more fragments are addressed is configured to reassembly overlapping fragments recited in [0051-0055]; [0089-0093]; Fig. 1-7, 10-11; [0019-0026]).

Regarding claim 16, performing further processing comprises determining whether the fragmented network traffic should be forwarded to the destination node (see 0051-0055]; [0089-0093]; Fig. 1-7, 10-11; [0019-0026]).

Regarding claim 18, wherein detecting an anomaly comprises determining that said two or more fragments overlap (see [0022]-[0026]).

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 7 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pochon et al. (US 2003/0048793), of record, in view of Motoyama et al. (US 2007/0124455).

Pochon discloses the claimed limitations above. Pochon does not explicitly disclose the following features: regarding claims 7 and 22, querying the destination node.

Motoyama discloses method and apparatus for providing multiple vendor support to remotely monitored devices comprising the following features.

Regarding claims 7 and 22, querying the destination node (see querying monitored device to obtain configuration information recited in [0022]; the abstract).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the method/ system/computer readable storage medium of Pochon by using features, as taught by Motoyama, in order to determine if the monitoring system is configured to interface with the monitored device using information stored in a first database and determine if the monitored device is supported by the monitoring system. See the abstract.

7. Claims 9-15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pochon et al. (US 2003/0048793), of record, in view of Cantrell et al. (US 2004/0093513).

Pochon disclosed the claimed limitations above. Pochon does not explicitly disclose the following features: regarding claim 10, processing the anomaly to determine whether the fragmented network traffic is associated with a threat; regarding claim 11, performing an action on the fragmented network traffic based on whether the fragmented network traffic is associated with a threat; regarding claim 12, discarding at least a portion of the fragmented network traffic if the fragmented network traffic is associated with a threat; regarding claim 13, copying one or more fragments comprising the fragmented network traffic to a buffer; regarding claim 14, performing further processing comprises sending an alert; regarding claim 15, performing further

processing comprises determining whether the fragmented network traffic should be blocked.

Cantrell discloses active network defense system and method comprising the following features.

Regarding claim 10, processing the anomaly to determine whether the fragmented network traffic is associated with a threat (see [0065]).

Regarding claim 11, performing an action on the fragmented network traffic based on whether the fragmented network traffic is associated with a threat (see [0063]).

Regarding claim 12, discarding at least a portion of the fragmented network traffic if the fragmented network traffic is associated with a threat (see [0063]).

Regarding claim 13, copying one or more fragments comprising the fragmented network traffic to a buffer (see [0065], where it is implicit that the traffic is copied to a buffer).

Regarding claim 14, performing further processing comprises sending an alert (see [0063]).

Regarding claim 15, performing further processing comprises determining whether the fragmented network traffic should be blocked (see [0063]).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the method/system/computer readable storage medium of Pochon by using features, as taught by Cantrell, in order to monitor and block traffic in an automated fashion, identify threats existing across multiple sessions and within

individual sessions, block threatening packet traffic and terminate threatening sessions, extract suspicious traffic from the data flow for further examination with more comprehensive content matching as well as asset risk analysis, and provide a flow control mechanism to control passage rate for packets passing through the data flow. See the abstract.

8. Claim 24 is rejected under 35 U.S.C. 103(a) as being unpatentable over Pochon et al. (US 2003/0048793), of record, in view of Ahmed et al. (US 2004/0083385).

Pochon discloses the claimed limitations above. Pochon does not explicitly disclose the following features: regarding claim 24, initiating in response to detecting said anomaly expanded buffering of fragments contained in said fragmented network traffic in response to detecting the anomaly.

Ahmed discloses dynamic network security apparatus and methods for network processors comprising the following features.

Regarding claim 24, initiating in response to detecting said anomaly expanded buffering of packets contained in the packet network traffic in response to detecting the anomaly (see increasing the size of the connection queue when detecting a TCP SYN attack recited in [0030]).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the method/system/computer readable storage medium of Pochon by using features, as taught by Ahmed, in order to dynamically load a security algorithm in a network processor based on network conditions (Ahmed: [0001]) and allow a more

careful examination of the suspicious packet to determine whether the packet is benign or malicious.

Response to Arguments

9. In the interview conducted on July 21, 2009. Examiner has stated that apparently the proposed amendment would over the previous Office Action. However, in further examination and consideration, examiner found new ground rejections for the instant application based on new interpretation of the claims.

10. Applicant's arguments filed 7/28/2009 have been fully considered but they are not persuasive. Applicant argued that Pochon does not disclose "performing a query to determine configuration information associated with how a destination node to which the two or more fragments are addressed is configured to reassemble overlapping fragments". In response to applicant's argument, the examiner respectfully disagrees with the argument. Pochon discloses performing a query to determine configuration information associated with how a destination node to which the two or more fragments are addressed is configured to reassemble overlapping fragments (see querying normalization table to determine information that is associated with how a end-system/host to which the two or more fragments are addressed is configured to reassembly overlapping fragments recited in [0051-0055]; [0089-0093]; Fig. 1-7, 10-11; [0019-0026]).

11. Applicant's arguments with respect to claims 7 and 22 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

12. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tung Q. Tran whose telephone number is (571) 272-9737. The examiner can normally be reached on Mon-Fri: 8:30 am - 6 pm, off alternative Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kwang B. Yao can be reached on (571) 272-3182. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Tung Q. Tran/
Examiner, Art Unit 2473

/KWANG B. YAO/

Supervisory Patent Examiner, Art Unit 2473